AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended) A method for managing network resources for externally authenticated users, the method comprising:
authenticating a user in a first administrative domain;
generating a token for the user, the token assigning at least a first role for the user, the first role identifying the user as a member of a pre-defined class of users; and
configuring the token to identify the user by the first role to a component of a second administrative domain; and
receiving a request from the user to retrieve network resources from the second administrative domain and;
determining whether the user is authorized to access the network resources of the second administrative domain based on the first role in the token.

2. (Original) The method of claim 1, wherein configuring the token to identify the user by the first role includes configuring the token to identify the user as the first role to the component of the second administrative domain without revealing a personal identification of the user to the component.

3. (Currently Amended) The method of claim 1, wherein configuring the token to identify the user by the first role includes configuring the token to identify the user by the first role to a policy server external to the first administrative domain, ~~thereby enabling~~ wherein the user is able to retrieve network resources from the second administrative domain according to a policy of the policy server.

4. (Currently Amended) A method as recited in claim 1,

~~wherein configuring the token to identify the user by the first role includes configuring the token to identify the user by the first role to a policy server external to the first administrative domain;~~

~~and further comprising the steps of:~~

~~receiving a request from the user to retrieve network resources from the second administrative domain;~~

wherein determining whether the user is authorized to access the network resources of the second administrative domain includes determining whether the user is authorized to access the network resources according to a policy of the policy server and based on the first role in the token.

5. (Original) The method of claim 1, wherein generating a token for the user includes assigning multiple roles for the user on the first token, each of the multiple roles being identifiable to a policy server external to the first administrative domain.

6. (Original) The method of claim 1, further comprising the steps of:

attaching the token to a terminal associated with the user;

automatically receiving the token at the second administrative domain when the user requests one or more resources from the second administrative domain.

7. (Original) The method of claim 1, further comprising the steps of:

attaching an indicator for the token to a terminal associated with the user;

automatically receiving the indicator to the component to inform the component of a location of the token on another computer.

8. (Original) The method of claim 1, wherein generating a token for the user includes providing information about a quality of authentication for the user.

9. (Original) The method of claim 1, wherein generating a token for the user includes providing information about a location of the user in the token.

10. (Original) The method of claim 1, wherein generating a token for the user includes providing information in the token about a personal identification of the user, a time stamp for when the token was generated, and the first role.

11. (Original) The method of claim 1, wherein generating a token for the user includes providing information in the token selected from a group of information consisting of information about a personal identification of the user, a time stamp for when the token was generated, and the first role; and further including the steps of encrypting at least some of the information in the token for use in the second administrative domain.

12. (Original) A method for managing network resources in multiple administrative domains, the method comprising:

in a first administrative domain:

authenticating a user in response to a request to access one or more resources in the first administrative domain;

generating a token for the user, the token assigning at least a first role to the user, the first role identifying the user as a member of a class of users;

in second administrative domain:

receiving a second request from the user to access one or more second resources in the second administrative domain, wherein the second request includes the token;

identifying a first policy for the first role specified by the token; and

managing access of the user to the second resources according to the first policy.

13. (Original) The method of claim 12, wherein managing the user according to the first policy includes checking the first policy to determine if an operation requested by the user for the second resources of the second administrative domain is permitted for the first role.

14. (Original) The method of claim 12, wherein managing the user according to the first policy includes checking the first policy to determine if an operation requested by the

user for the second resources of the second administrative domain is permitted for the first role.

15. (Original) The method of claim 12, wherein managing the user according to the first policy includes checking the first policy to determine if an operation requested by the user for the second resources of the second administrative domain is permitted for the first role, and wherein the method further comprises allowing execution of the operation on the second resources only if the policy permits for the operation to be performed by any user assigned the first role.

16. (Original) The method of claim 12, wherein managing the user according to the first policy includes checking the first policy to determine if an operation requested by the user for the second resources of the second administrative domain is permitted for the first role, and wherein the method further comprises allowing execution of the operation on the second resources only if the policy permits for the operation to be performed by any user assigned the first role.

17. (Original) The method of claim 12, wherein managing the user according to the first policy includes identifying an allowable time period in which any user assigned the first role can access the second resources of the second administrative domain, and wherein the method further includes determining if the user is accessing the second resources of the second administrative domain during the allowable time period

18. (Currently Amended) A method for managing network resources for externally authenticated users, the method comprising:

receiving a first request to authenticate a user in a first administrative domain;

authenticating [[a]] the user in [[a]] the first administrative domain;

generating a token for the user, wherein the token includes information defining a first role for the user, wherein the first role identifies the user as a member of a pre-defined class of users;

receiving a second request from the user to access one or more network resources located in a second administrative domain; and determining whether to grant the user access to the network resources based on the role in the token and without re-authenticating the user in the second administrative domain.

19. (Cancelled).

20. (Cancelled)

21. (Cancelled).

22. (Cancelled)

23. (Currently Amended) A computer system for managing network resources, the computer system comprising:

a storage medium that stores identification information for users that access the network;

processing resources located in a first administrative domain, the processing resources being configured to:

~~access the storage medium to identify~~ authenticating a user ~~accessing the network~~ in the first administrative domain;

generate a token for the user in response to the user ~~accessing the network~~, the token identifying at least a first role for the user and identifying the user as a member of a pre-defined class of users; and

configure the token to enable the user to be identified by the first role in a second administrative domain, ~~so that~~ wherein the user is provided access to a resource of the second administrative domain according to a policy for the first role;

receiving a request from the user to retrieve network resources from the second administrative domain;

determining whether the user is authorized to access the network resources of the second administrative domain based on the first role in the token.

24. (Original) The computer system of claim 23, wherein the processing resource is configured to authenticate the user by accessing the identification information in the first storage medium.

25. (Original) The computer system of claim 23, wherein the processing resources is configured to associate the token with the user for a duration when the terminal of the user is connected to the network.

26. (Original) The computer system of claim 23, wherein the token expires after the terminal is disconnected from the network.

27. (Cancelled)

28. (Cancelled)

29. (Cancelled)

30. (Currently Amended) A computer-readable medium for managing network resources in multiple administrative domains, the computer-readable medium carrying instructions for performing the steps of:

assigning at least a first role to a plurality of users that access a first administrative domain; and

causing each of the plurality of users to be identified by the first role on a component of the second administrative domain, ~~so that~~ wherein the first role identifies a policy that is shared by the plurality of users for accessing resources managed in the second administrative domain.

receiving a request from the user to retrieve network resources from the second administrative domain and;

determining whether the user is authorized to access the network resources of the second administrative domain based on the first role in the token.

31. (Original) The computer-readable medium of claim 30, further comprising instructions for authenticating the plurality of users in a first administrative domain before assigning at least a first role to the plurality of users.

32. (Original) The computer-readable medium of claim 30, further comprising assigning at least the first role to a plurality of users during a network session between each of the users and the first administrative domain, and causing each of the plurality of users to be identified by the first role after each of the plurality of users selects to access the second administrative domain during the network session.

33. (Original) The computer-readable medium of claim 30, further comprising assigning at least a first role to a plurality of users includes generating a token that identifies the first role to a policy server of the second administrative domain.

34. (Cancelled)